New Results on Secret Key Establishment over a Pair of Broadcast Channels

Hadi Ahmadi, Reihaneh Safavi-Naini
Department of Computer Science, University of Calgary, Canada.
{hahmadi, rei}@ucalgary.ca

Abstract

The problem of Secret Key Establishment (SKE) over a pair of independent Discrete Memoryless Broadcast Channels (DMBCs) has already been studied in [3], where we provided lower and upper bounds on the secret-key capacity. In this paper, we study the above setup under each of the following two cases: (1) the DMBCs have secrecy potential, and (2) the DMBCs are stochastically degraded with independent channels. In the former case, we propose a simple SKE protocol based on a novel technique, called Interactive Channel Coding (ICC), and prove that it achieves the lower bound. In the latter case, we give a simplified expression for the lower bound and prove a single-letter capacity formula under the condition that one of the legitimate parties can only send i.i.d. variables.

I. Introduction

We consider the following problem of Secret Key Establishment (SKE): Alice and Bob want to share a secret key in the presence of an eavesdropping adversary, Eve. Information-theoretic solutions to this problem assume that a collection of sources and/or channels are available to the parties. We refer this as a *setup*.

Wyner's pioneering work [14] and its generalization by Csiszár and Körner [4] considered transmission of secure messages over a Discrete Memoryless Broadcast Channel (DMBC) from Alice to Bob and Eve. They defined the secrecy capacity in this setup as the highest rate of secure and reliable message transmission (in bits per channel use) and showed that this capacity is positive if Bob's channel is less noisy [8] than Eve's. The work in [4], [14] has also been proved for the case of Gaussian channels [10]. These results can also be used for SKE since any secure message transmission protocol can be used to send a secret-key securely over the DMBC.

Extensions of the work in [4], [14] have investigated the improvement of SKE by considering new setups. Maurer [11] and independently Ahlswede and Csiszár [1] studied SKE when there is a DMBC from Alice to Bob and Eve, and a public discussion channel between Alice and Bob that is reliable, insecure, and unlimitedly available in both directions. They also considered SKE when the DMBC above is replaced by a Discrete Memoryless Multiple Source (DMMS) between the parties. Csiszár and Narayan [5] considered SKE in the latter setup with a slight difference that the public channel is one-way and limited in rate. Ahlswede and Cai [2] studied SKE when Wyner's setup is accompanied by an additional secure (and reliable) *output feedback channel* that is used to feed back the information received from the forward channel. Noisy feedback over modulo-additive broadcast channels is another extension [9], [13]. Khisti et al. [7] and independently Prabhakaran et al. [12] considered a setup where the parties have access to a DMMS and a DMBC from Alice to Bob and Eve.

In practice special types of channel, e.g., public discussion channel, must be realized from more basic resources such as a DMBC. In [3], we introduced a new setup for SKE, called *2DMBC*, where the only resources available to Alice and Bob are two independent DMBCs in the two directions. This setup is appropriate to model wireless networks where two nodes can communicate interactively and their communication is eavesdropped by their wireless neighbors. The secret-key capacity in this setup is defined as the maximum rate of secure and reliable key establishment, in bits per channel use. Lower and upper bounds on the secret-key capacity in the 2DMBC setup have been provided and shown to coincide when the broadcast channels are *physically degraded* [3].

A. Our work

Motivated by applying the theoretical results to practical communication scenarios, in this paper, we extend the results of [3] in the following directions.

1) We consider the 2DMBC setup when both DMBCs have *secrecy potential*, by which, we mean that realizing a noiseless channel from any of the DMBCs is not optimal. In most of the channels of interest (in communication), this occurs when the DMBCs have non-zero secrecy capacities. We propose a two-round SKE protocol based on a novel technique, called *Interactive Channel Coding (ICC)* that achieves the lower bound in [3]. This lower bound was proved before by a SKE protocol that, although being convenient for the proof, uses an elaborate two-level coding construction whose efficient design becomes a new challenge in practice. Instead, ICC is a simple extension of systematic channel coding to a two-round construction in which the messages are essentially a codeword from a systematic error correcting code, split into two parts: one received in the first round and one sent in the second round. Roughly speaking, the ICC protocol works as follows. Alice sends a random sequence R_A and Bob receives a noisy version of it, I_A. He chooses an independent random sequence, I_B, and appends it to I_A. We refer to the concatenated sequence $I = (I_A||I_B)$ as the *information sequence*. Bob uses his systematic encoder to calculate a *parity-check sequence* P for the information sequence I, and sends $(I_B||P)$ to Alice, where Alice receives $(R_B||R_P)$. She uses her systematic decoder to decode $R = (R_A||R_B||R_P)$ to $\hat{I} = (\hat{I}_A||\hat{I}_B)$ as an estimation of the information sequence. The rest is to generate a secure key from the information sequence. ICC is particularly important as it allows progress in systematic capacity achieving codes to be directly applied to SKE.

2) We study the 2DMBC setup when the DMBCs are *stochastically degraded with independent channels*. We refer to this setup as *sd-2DMBC*. This study is motivated by observing that the results in [3] for the secret-key capacity of (physically) degraded 2DMBCs do not necessarily hold for stochastically degraded 2DMBCs. In setups like [4], [5], [7], [12] that do not offer interactive communication, physically and stochastically degraded broadcast channels are equivalent in terms of the secret-key capacity. This is not true, however, for the 2DMBC setup in which interactive communication is permitted. Two important classes of stochastically degraded channels with independent components are binary symmetric broadcast channels and Gaussian broadcast channels. We note that our results can be easily extended to continuous memoryless channels.

2-a) We give a simplified expression for the lower bound on the secret-key capacity in the sd-2DMBC setup which uses fewer random variables and hence results in a simpler maximization problem.

2-b) We consider sd-2DMBC when one of the parties can only send only independently, identically distributed (i.i.d) variables. We prove a single-letter formula for the secret-key capacity that is achieved by a two-round protocol.

An example of the scenario (2-b) is when a base station wants to establish keys with several users in different locations. The offline computation power of the base station is high but its realtime computation power is limited. So, the base station sends i.i.d. variables in realtime and stores the received variables from all other nodes in all communication rounds. Next, it calculates the common keys with each user from the stored information in the offline mode. Our study of the above scenario provides a solution to this problem.

B. Notation

We use calligraphic letters $(\mathcal{U})$ to denote finite alphabets (sets), and the corresponding letters in uppercase (U) and lowercase (u) to denote random variables (RVs) and their realizations, respectively. The size of $\mathcal{U}$ is denoted by $|\mathcal{U}|$. $\mathcal{U}^n$ is set of all sequences of length n whose elements are in $\mathcal{U}$; $U^n = (U_1, U_2, \ldots, U_n)$ is called an n-sequence, i.e., a sequence of n (possibly correlated) RVs in $\mathcal{U}$, and U_i^j is used to denote a part of this sequence that is $(U_i, U_{i+1}, \ldots, U_j)$. We use '$||$' to show the concatenation of sequences. For a value x, we use $[x]_+$ to show $\max\{0, x\}$. For three random sequences Q_1, Q_2, and Q_3, we use $Q_1 \leftrightarrow Q_2 \leftrightarrow Q_3$ to denote a Markov chain between them in this order.

C. Paper organization

Section II describes the 2DMBC setup, definitions, and existing SKE results in this setup. Section III summarizes the main results of this paper. Section IV is dedicated to the proofs. We conclude the paper in Section V.

II. Model, Definitions, and Existing Results

The 2DMBC setup is depicted in Fig. 1. There is a forward DMBC, $X_f \to (Y_f, Z_f)$ specified by $P_{Y_f,Z_f|X_f}$, from Alice to Bob (and Eve) and a backward DMBC, $X_b \to (Y_b, Z_b)$ specified by $P_{Y_b,Z_b|X_b}$, from Bob to Alice (and Eve). We assume that each party has free access to an independent source of randomness.

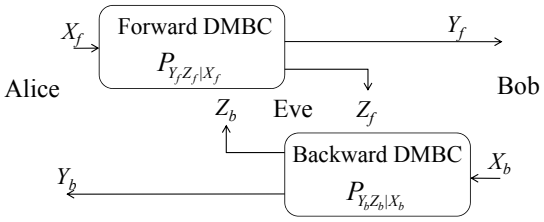


Fig. 1. The 2DMBC setup

An SKE protocol in this setup may contain several communication rounds. In each round either Alice or Bob sends a sequence of random variables (RVs) which is computed using some independent randomness and the communicated (sent and/or received) sequences in the previous rounds. Finally each party will

have a set of communicated sequences, which form their *view*. Using their views, one of the legitimate parties computes a key S, and the other one computes an estimation of the key $\hat{S}$. A secure SKE protocol and the secret-key capacity in the 2DMBC setup are defined as follows.

Definition 1: [3] An SKE protocol Π in the 2DMBC setup is (R_{sk}, δ)-*secure* if it results in the key S and its estimation $\hat{S}$ such that

$$\frac{H(S)}{n_f + n_b} > R_{sk} - \delta, \tag{1a}$$

$$\Pr(\hat{S} \neq S) < \delta, \tag{1b}$$

$$\frac{H(S|View_E)}{H(S)} > 1 - \delta, \tag{1c}$$

where $View_E$ is Eve's view at the end of the protocol, and n_f and n_b are the number of times that the forward and the backward channels are used, respectively.

Definition 2: [3] The *secret-key capacity* in the 2DMBC setup, C_{sk}^{2DMBC}, is the largest $R_{sk} \geq 0$ such that, for any arbitrarily small $\delta > 0$, there exists an (R_{sk}, δ)-secure SKE protocol.

We recall the lower and the upper bounds given in [3] on the secret-key capacity in the 2DMBC setup. Let the RVs X_f, Y_f, Z_f (resp. X_b, Y_b, Z_b) correspond to the conditional distribution $P_{Y_f,Z_f|X_f}$ (resp. $P_{Y_b,Z_b|X_b}$), specified by the 2DMBC. Let V_f, V_b, $W_{1,f}, W_{2,f}$, $W_{1,b}, W_{2,b}$ be RVs from arbitrary sets where V_f, V_b, $(W_{1,f}, W_{2,f})$, and $(W_{1,b}, W_{2,b})$ are independent and the following Markov chains are satisfied:

$$V_f \leftrightarrow Y_f \leftrightarrow (X_f, Z_f),\ W_{2,b} \leftrightarrow W_{1,b} \leftrightarrow X_b \leftrightarrow (Y_b, Z_b), \tag{2a}$$

$$V_b \leftrightarrow Y_b \leftrightarrow (X_b, Z_b),\ W_{2,f} \leftrightarrow W_{1,f} \leftrightarrow X_f \leftrightarrow (Y_f, Z_f). \tag{2b}$$

Also let

$$R_{s1}^A = I(V_f; X_f) - I(V_f; Z_f), \tag{3a}$$

$$R_{s2}^A = I(W_{1,b}; Y_b|W_{2,b}) - I(W_{1,b}; Z_b|W_{2,b}), \tag{3b}$$

$$R_{s1}^B = I(V_b; X_b) - I(V_b; Z_f), \tag{3c}$$

$$R_{s2}^B = I(W_{1,f}; Y_f|W_{2,f}) - I(W_{1,f}; Z_f|W_{2,f}). \tag{3d}$$

The secret-key capacity is lower bounded [3] as

$$C_{sk}^{2DMBC} \geq \max\{L_A, L_B\}, \tag{4}$$

where

$$L_A = \max_{n_f, n_b, P_{X_f,V_f}, P_{X_b,W_{2,b},W_{1,b}}} \left[\frac{n_f R_{s1}^A + n_b [R_{s2}^A]_+}{n_f + n_b} \text{s. t. } \ n_f I(V_f; Y_f|X_f) < n_b I(W_{1,b}; Y_b) \right], \tag{5}$$

$$L_B = \max_{n_f, n_b, P_{X_b,V_b}, P_{X_f,W_{2,f},W_{1,f}}} \left[\frac{n_b R_{s1}^B + n_f [R_{s2}^B]_+}{n_f + n_b} \text{s. t. } \ n_b I(V_b; Y_b|X_b) < n_f I(W_{1,f}; Y_f) \right], \tag{6}$$

and it is upper bounded [3] as

$$C_{sk}^{2DMBC} \leq \max_{P_{X_f}, P_{X_b}} \{I(X_f; Y_f|Z_f), I(X_b; Y_b|Z_b)\}. \tag{7}$$

III. Statement of Main Results

A. The interactive channel coding protocol

The lower bound in (4) has been obtained by an SKE protocol [3] that uses a complicated two-level coding construction whose efficient design becomes a challenge in practice. We introduce the interactive channel coding (ICC) technique which is used to design the so-called *ICC protocol* for SKE. We show that when the DMBCs have secrecy potential, the ICC protocol can achieve the lower bound in (4). ICC relies on the existence of capacity-achieving *systematic channel codes*. Designing efficient constructions for systematic channel codes has been well studied, e.g., a large body of work on the design of capacity achieving channel codes follows on linear block codes which can be represented as systematic codes. This makes the design of an efficient ICC protocol for SKE as simple as the design of efficient coding for SKE over a (one-way) DMBC [4].

Definition 3: A *(bipartite) systematic channel code*, with encoding alphabets $(\mathcal{Y}_f, \mathcal{X}_b)$ and decoding alphabets $(\mathcal{X}_f, \mathcal{Y}_b)$, is specified by a pair of encoding/decoding functions (Enc/Dec), where

- $Enc : \mathcal{Y}_f^{n_f} \times \mathcal{X}_b^{n_{b,i}} \to \mathcal{Y}_f^{n_f} \times \mathcal{X}_b^{n_b}$ deterministically maps $(y_f^{n_f}||x_b^{n_{b,i}})$ (as the information sequence) to the codeword $(y_f^{n_f}||x_b^{n_b})$ such that $x_b^{n_b} = (x_b^{n_{b,i}}||x_b^{n_{b,p}})$ and $n_b = n_{b,i} + n_{b,p}$; we call $x_b^{n_{b,p}}$ the parity-check sequence.
- $Dec : \mathcal{X}_f^{n_f} \times \mathcal{Y}_b^{n_b} \to \mathcal{Y}_f^{n_f} \times \mathcal{X}_b^{n_{b,i}}$ deterministically assigns a guess $(\hat{y}_f^{n_f}||\hat{x}_b^{n_{b,i}})$ to each input $(x_f^{n_f}||y_b^{n_b})$.

The general construction of the ICC protocol and a proof of Theorem 1 are provided in Section IV-A. In the following, we describe the ICC protocol for a special case when $V_f = Y_f$, $W_{2,b} = 1$, $W_{1,b} = X_b$, and Alice is the initiator (see Fig. 2). Accordingly, we rephrase the argument to be maximized and the constraint condition in (12) respectively as

$$R_{sk} = \frac{n_f[I(Y_f;X_f) - I(Y_f;Z_f)] + n_b[I(X_b;Y_b) - I(X_b;Z_b)]}{n_f + n_b}, \tag{8}$$

$$n_f(H(Y_f|X_f) + \alpha) \le n_b I(X_b;Y_b), \tag{9}$$

where $\alpha > 0$ is an arbitrarily small constant. Let $n_b = n_{b,i} + n_{b,p}$, where $n_{b,i}$ is chosen to satisfy

$$n_{b,i} H(X_b) = n_b I(X_b;Y_b) - n_f(H(Y_f|X_f) + \alpha). \tag{10}$$

Let $N = n_f + n_b$ and ϵ be a small constant such that $5N\epsilon < n_f\alpha$. Let $\mathcal{Y}_{f,\epsilon}^{n_f}$ (resp. $\mathcal{X}_{b,\epsilon}^{n_{b,i}}$) be the set of all ϵ-typical sequences w.r.t. P_{Y_f} (resp. P_{X_b}) in $\mathcal{Y}_f^{n_f}$ (resp. $\mathcal{X}_b^{n_{b,i}}$); Define

$$\eta_f = \log|\mathcal{Y}_{f,\epsilon}^{n_f}|, \qquad \eta_b = \log|\mathcal{X}_{b,\epsilon}^{n_{b,i}}|,$$
$$\eta = \eta_f + \eta_b, \qquad \kappa = NR_{sk}, \qquad \gamma = \eta - \kappa.$$

Let $\{\mathcal{G}_i\}_{i=1}^{2^\kappa}$ be a partition of $\mathcal{Y}_{f,\epsilon}^{n_f} \times \mathcal{X}_{b,\epsilon}^{n_{b,i}}$ into 2^κ parts, each of size 2^γ. Define $g : \mathcal{Y}_{f,\epsilon}^{n_f} \times \mathcal{X}_{b,\epsilon}^{n_{b,i}} \to \{1, 2, \ldots, 2^\kappa\}$ as a function that, for every input $(y_f^{n_f}, x_b^{n_{b,i}}) \in \mathcal{G}_i$, outputs i.

Encoding. Alice chooses an i.i.d. n_f-vector $X_f^{n_f}$ and sends it over the forward DMBC; Bob and Eve receive $Y_f^{n_f}$ and $Z_f^{n_f}$, respectively. If $Y_f^{n_f} \notin \mathcal{Y}_{f,\epsilon}^{n_f}$, Bob returns a NULL; otherwise, he chooses uniformly at random an $n_{b,i}$-sequence $X_b^{n_{b,i}}$ from $\mathcal{X}_{b,\epsilon}^{n_{b,i}}$, encodes $Enc(Y_f^{n_f}||X_b^{n_{b,i}}) = (Y_f^{n_f}||X_b^{n_b})$, and sends $X_b^{n_b}$ over the backward DMBC; Alice and Eve receive $Y_b^{n_b}$ and $Z_b^{n_b}$, respectively.

Decoding. Alice decodes $(\hat{Y_f}^{n_f}||\hat{X}_b^{n_{b,i}}) = Dec(X_f^{n_f}||Y_b^{n_b})$ using bipartite jointly typical decoding: she searches through the 2^η words in $\mathcal{Y}_{f,\epsilon}^{n_f} \times \mathcal{X}_{b,\epsilon}^{n_{b,i}}$ and either finds a unique $(\hat{Y}_f^{n_f}, \hat{X}_b^{n_{b,i}})$ such that $Enc(\hat{Y}_f^{n_f}, \hat{X}_b^{n_{b,i}})$

and $(X_f^{n_f}, Y_b^{n_b})$ are (n_f, ϵ)-bipartite jointly typical w.r.t. $(P_{Y_f,X_f}, P_{X_b,Y_b})$ (see Section IV-A, Definition 7), or returns a NULL.

Key derivation. Bob computes $S = g(Y_f^{n_f}, X_b^{n_{b,i}})$. Alice computes $\hat{S} = g(\hat{Y_f}^{n_f}, \hat{X}_b^{n_{b,i}})$.

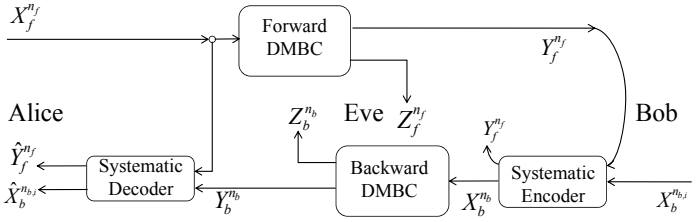


Fig. 2. ICC over a 2DMBC: Alice initiates the protocol

Theorem 1: Taking the variables from (2) and (3), the ICC protocol can achieve the secret-key rate

$$R^{ICC} = \max\{R_A^{ICC}, R_B^{ICC}\}, \tag{11}$$

where

$$R_A^{ICC} = \max_{n_f,n_b,P_{X_f,V_f},P_{X_b,W_{2,b},W_{1,b}}} \{\frac{n_f R_{s1}^A + n_b R_{s2}^A}{n_f + n_b} \text{ s. t. } n_f[I(V_f;Y_f|X_f)] < n_b I(W_{1,b};Y_b)\}, \tag{12}$$

$$R_B^{ICC} = \max_{n_f,n_b,P_{X_b,V_b},P_{X_f,W_{2,f},W_{1,f}}} \{\frac{n_f R_{s1}^B + n_b R_{s2}^B}{n_f + n_b} \text{ s. t. } n_b[I(V_b;Y_b|X_b)] < n_f I(W_{1,f};Y_f)\}. \tag{13}$$

Comparing (5) with (12), we conclude that R_A^{ICC} and L^A are equal if for the optimal selection of the parameters, in the maximization problem of (5), R_{s2}^A becomes non-negative. In other words, the two values (rates) are equal if the backward DMBC has secrecy potential, i.e., the optimal strategy is not based on realizing a noiseless channel from the backward DMBC. Similarly, R_B^{ICC} equals L^B if the forward DMBC has secrecy potential.

Corollary 1: When the DMBCs have secrecy potential, the ICC protocol can achieve the lower bound in (4).

B. The secret-key capacity in the sd-2DMBC setup

SKE over *physically degraded* 2DMBCs (pd-2DMBCs) was considered in [3], where we showed that the lower and the upper bounds coincide and the capacity is achieved by a one-round SKE protocol. This implies that interaction over a pd-2DMBC cannot increase the SKE rate. However, this is not generally true for *stochastically degraded* broadcast channels, and the upper bound in (7) does not necessarily coincide with the lower bound in (4) for stochastically degraded DMBCs. In this paper, we consider SKE over a 2DMBC, where each DMBC is *stochastically degraded with independent channels*. We refer to this setup as *sd-2DMBC*.

Definition 4: The DMBC $X \to (Y, Z)$, with conditional distribution $P_{YZ|X}$, is *stochastically degraded in favor of* Y (or the party who receives Y) if there exist two RVs $\tilde{Y}$ and $\tilde{Z}$ such that $X \leftrightarrow \tilde{Y} \leftrightarrow \tilde{Z}$ forms a Markov chain and

$$P_{XY}(x,y) = P_{X,\tilde{Y}}(x,y), \qquad P_{XZ}(x,z) = P_{X,\tilde{Z}}(x,z).$$

It consists of *independent channels* if $P_{YZ|X} = P_{Y|X}.P_{Z|X}$.

Definition 5: A *sd-2DMBC* is a 2DMBC whose DMBCs are stochastically degraded (either in favor of Y or in favor of Z), and consist of independent channels.

1) Lower bound:

Proposition 1: The secret-key capacity in the sd-2DMBC setup is lower bounded as

$$C_{sk}^{sd-2DMBC} \geq \max\{L'_A, L'_B\}, \tag{14}$$

where

$$L'_A = \max_{n_f, n_b, P_{V_f, X_f, X_b}} \{\frac{n_f I(V_f; X_f|Z_f) + n_b[I(X_b; Y_b) - I(X_b; Z_b)]_+}{n_f + n_b} \text{ s. t. } n_f[I(V_f; Y_f|X_f)] < n_b I(X_b; Y_b)\}, \tag{15}$$

$$L'_B = \max_{n_f, n_b, P_{V_b, X_b, X_f}} \{\frac{n_b I(V_b; X_b|Z_b) + n_f[I(X_f; Y_f) - I(X_f; Z_f)]_+}{n_f + n_b} \text{ s. t. } n_b[I(V_b; Y_b|X_b)] < n_f I(X_f; Y_f)\}. \tag{16}$$

The expressions (15) and (16) do not contain the RVs $W_{1,b}, W_{2,b}, W_{1,f}$, and $W_{2,f}$, compared to (5) and (6). So, the maximization problem in obtaining the lower bound (14) is easier than that in (4).

2) single-letter characterization: We consider a scenario where one of the legitimate parties can only send i.i.d. variables, and derive an expression for the secret-key capacity under this condition.

Theorem 2: When one of the legitimate parties can only send i.i.d. variables, the secret-key capacity in the sd-2DMBC setup equals

$$\max\{L'_A, L'_B\}, \tag{17}$$

where L'_A and L'_B are given in (15) and (16), respectively.

IV. Proofs

A. Proof of Theorem 1, the ICC protocol

We describe the ICC protocol when Alice is the initiator and prove that it achieves the rate in (12). In a similar way, one can describe ICC when Bob initiates the protocol and prove (13). First we give the following definitions from [3] for *bipartite typical sequences*. A bipartite sequence $X^N = (U^n||T^d)$, where $N = n+d$, is the concatenation of two subsequences, $U^n \in \mathcal{U}^n$ and $T^d \in \mathcal{T}^d$, with two probability distributions, P_{U^n} and P_{T^d}, respectively.

Definition 6: A sequence $x^N = (u^n||t^d)$ is an (ϵ, n)*-bipartite typical sequence* with respect to the probability distribution pair $(P_U(u), P_T(t))$, iff

$$|-\frac{1}{N}\log P(x^N) - \frac{nH(U) + dH(T)}{N}| < \epsilon, \tag{18}$$

where $P(x^N)$ is calculated as

$$P(x^N) = \prod_{i=1}^{n} P_U(u_i) \times \prod_{i=1}^{d} P_T(t_i). \tag{19}$$

Definition 7: A pair of sequences $(x^N, y^N) = ((u^n||t^d), (u'^n||t'^d))$ is an (ϵ, n)*-bipartite jointly typical pair of sequences* with respect to the probability distribution pair $(P_{U,U'}(u, u'), P_{T,T'}(t, t'))$, iff x^N

and y^N are (ϵ, n)-bipartite typical sequences with respect to the marginal probability distribution pairs $(P_U(u), P_T(t))$ and $(P_{U'}(u'), P'_T(t'))$, respectively, and

$$|-\frac{1}{N}\log P(x^N, y^N) - \frac{nH(U,U') + dH(T,T')}{N}| < \epsilon, \tag{20}$$

where $P(x^N, y^N)$ is calculated as

$$P(x^N, y^N) = \prod_{i=1}^{n} P_{U,U'}(u_i, u'_i) \times \prod_{i=1}^{d} P_{T,T'}(t_i, t'_i). \tag{21}$$

Back to the proof, let the RVs V_f, X_f, Y_f, Z_f, and $W_{1,b}, W_{2,b}, X_b, Y_b, Z_b$ be the same as defined in Theorem 1 such that the Markov chains in (2) are satisfied. Also let n_f and n_b be integers that satisfy the constraint condition in (12). For simplicity, we use W_1, W_2, and V to refer to $W_{1,b}, W_{2,b}$, and V_f, respectively. Accordingly, we write the argument to be maximized in (12) as

$$R_{sk} = \frac{n_f R^A_{s1} + n_b R^A_{s2}}{n_f + n_b} \tag{22}$$

where

$$R^A_{s1} = I(V; X_f) - I(V; Z_f), \tag{23a}$$

$$R^A_{s2} = I(W_1; Y_b|W_2) - I(W_1; Z_b|W_2), \tag{23b}$$

and we rephrase the constraint condition in (12) as

$$n_b I(W_1; Y_b) \geq n_f(I(V; Y_f|X_f) + 3\alpha), \tag{24}$$

where $\alpha > 0$ is an small constant to be determined (later) from δ. We shall show that for any given $\delta > 0$, for sufficiently large n_f and n_b that satisfy (24), the three requirements in (1) can be satisfied.

Let $N = n_f + n_b$ and $\epsilon, \beta > 0$ be small constants determined from α such that $3N\epsilon < n_b\beta = n_f\alpha$. Let $n_b = n_{b,1} + n_{b,2}$, where $n_{b,2}$ is chosen to satisfy

$$n_{b,2} I(W_1; Y_b) = n_f(I(V; Y_f|X_f) + 3\alpha). \tag{25}$$

Define

$$\eta_f = n_f[I(V; Y_f) + \alpha], \qquad \eta_{f,2} = n_{b,2} I(W_2; Y_b), \qquad \eta_{f,1} = \eta_f - \eta_{f,2}, \tag{26}$$

$$\eta_b = n_{b,1}[I(W_1; Y_b) - \beta], \qquad \eta_{b,2} = n_{b,1} I(W_2; Y_b), \qquad \eta_{b,1} = \eta_b - \eta_{b,2}, \tag{27}$$

$$\eta_1 = \eta_{f,1} + \eta_{b,1}, \qquad \eta_2 = \eta_{f,2} + \eta_{b,2}, \qquad \eta = \eta_f + \eta_b, \tag{28}$$

$$\kappa = (n_f + n_b)R_{sk}, \qquad \gamma = \eta - \kappa. \tag{29}$$

Although the quantities obtained in (25)-(29) are real values, for sufficiently large n_b and n_f, we can approximate them by integers. Since β can be made arbitrarily small, we can assume η_b and η_f are non-negative. Furthermore, since

$$\begin{aligned}
\eta = \eta_f + \eta_b &\overset{(a)}{=} n_f[I(V; Y_f, X_f) + \alpha] + n_{b,1}[I(W_1, Y_b) - \beta] \\
&= n_f I(V; X_f) + n_f I(V; Y_f|X_f) + n_f\alpha + n_{b,1} I(W_1, Y_b) - n_{b,1}\beta \\
&\overset{(b)}{=} n_f I(V; X_f) + n_{b,2} I(W_1, Y_b) - 2n_f\alpha + n_{b,1} I(W_1, Y_b) - n_{b,1}\beta \\
&\geq n_f I(V; X_f) + n_b I(W_1, Y_b) - 3n_f\alpha \geq R^A_{s1} + R^A_{s2} - 3n_f\alpha \\
&\geq \kappa - 3n_f\alpha,
\end{aligned}$$

for arbitrarily small α, we can assume $\eta \geq \kappa$ and so γ is non-negative. Equality (a) above is due to (26), (27), and the Markov chain $X_f \leftrightarrow Y_f \leftrightarrow V$, and equality (b) follows from (25). The following sets and functions are used in the design of the ICC protocol.

(i) $\mathcal{V}^{n_f}$ is the set of all possible n_f-sequences with elements from $\mathcal{V}$. Create $\mathcal{V}_\epsilon^{n_f}$ by randomly and independently selecting 2^{η_f} ϵ-typical sequences (w.r.t. P_V) from $\mathcal{V}^{n_f}$.

(ii) Let $\mathfrak{f} : \mathcal{V}_\epsilon^{n_f} \to \mathcal{F} = \{1, 2, \ldots, 2^{\eta_f}\}$ be an arbitrary bijective mapping; denote its inverse by $\mathfrak{f}^{-1}$.

(iii) let $\{\mathcal{F}_i\}_{i=1}^{2^{\eta_{f,2}}}$ be a partition of $\mathcal{F}$, into $2^{\eta_{f,2}}$ equal-sized parts. Label elements of part i as $\mathcal{F}_i = \{f_{i,j}\}_{j=1}^{\eta_{f,1}}$. Define $\mathfrak{f}_{\mathfrak{ind}} : \mathcal{F} \to \{1, \ldots, 2^{\eta_{f,2}}\} \times \{1, \ldots, 2^{\eta_{f,1}}\}$ such that $\mathfrak{f}_{\mathfrak{ind}}(f) = (i, j)$, if f is labeled by $f_{i,j}$.

(iv) $\mathcal{W}_1^{n_{b,1}}$ is the set of all possible sequences $W_1^{n_{b,1}}$. Create $\mathcal{W}_{1,\epsilon}^{n_{b,1}}$ by randomly selecting 2^{η_b} different ϵ-typical sequences (w.r.t. P_{W_1}) from $\mathcal{W}_1^{n_{b,1}}$.

(v) Let $\mathfrak{b} : \mathcal{W}_{1,\epsilon}^{n_{b,1}} \to \mathcal{B} = \{1, 2, \ldots, 2^{\eta_b}\}$ be an arbitrary bijective mapping; denote its inverse by $\mathfrak{b}^{-1}$.

(vi) In analogy to $\mathcal{F}$, let $\{\mathcal{B}_i\}_{i=1}^{2^{\eta_{b,2}}}$ be a partition of $\mathcal{B}$ where $\mathcal{B}_i = \{b_{i,j}\}_{j=1}^{2^{\eta_{b,1}}}$. Define $\mathfrak{b}_{indx} : \mathcal{B} \to \{1, \ldots, 2^{\eta_{b,2}}\} \times \{1, \ldots, 2^{\eta_{b,1}}\}$ such that $\mathfrak{b}_{indx}(b) = (i, j)$, if b is labeled by $b_{i,j}$.

(vii) Let $\{\mathcal{G}_i\}_{i=1}^{2^\kappa}$ be a partition of $\mathcal{F} \times \mathcal{B}$ into parts of size 2^γ. Define $g : \mathcal{F} \times \mathcal{B} \to \{1, 2, \ldots, 2^\kappa\}$ such that, for any input in $\mathcal{G}_i$, it outputs i.

(viii) Define the parity-check book $\mathcal{P}_2$ as a the collection of 2^{η_2} words $\{w_{2,f_2,b_2}^{n_{b,2}} : f_2 = 1, 2, \ldots, 2^{\eta_{f,2}},\ b_2 = 1, 2, \ldots, 2^{\eta_{b,2}}\}$, where each codeword $w_{2,f_2,b_2}^{n_{b,2}}$ is of length $n_{b,2}$ and is independently generated according to the distribution

$$\prod_{i=1}^{n_{b,2}} p(W_2 = w_{2,f_2,b_2}(i)).$$

(ix) For each $w_{2,f_2,b_2}^{n_{b,2}}$, Define the parity-check book $\mathcal{P}_1(w_{2,f_2,b_2}^{n_{b,2}})$ as a the collection of 2^{η_1} words $\{w_{1,f_2,b_2,f_1,b_1}^{n_{b,2}} : f_1 = 1, \ldots, 2^{\eta_{f,1}},\ b_1 = 1, \ldots, 2^{\eta_{b,1}}\}$, where each codeword $w_{1,f_2,b_2,f_1,b_1}^{n_{b,2}}$ is of length $n_{b,2}$ and is independently generated according to the distribution

$$\prod_{i=1}^{n_{b,2}} p(W_1 = w_{1,f_2,b_2,f_1,b_1}(i) | W_2 = w_{2,f_2,b_2}(i)).$$

(x) Let $Enc : \mathcal{V}^{n_f} \times \mathcal{W}_1^{n_{b,1}} \to \mathcal{V}^{n_f} \times \mathcal{W}_1^{n_b}$ be a (bipartite) systematic encoding function such that $Enc(v^{n_f}, w_1^{n_{b,1}}) = (v^{n_f}, w_1^{n_b})$, where $w_1^{n_b} = (w_1^{n_{b,1}}, w_{1,f_2,b_2,f_1,b_1}^{n_{b,2}})$, using the above parity-check books when $f = \mathfrak{f}(v^{n_f})$, $b = \mathfrak{b}(\mathcal{W}_1^{n_{b,1}})$, $(f_2, f_1) = \mathfrak{f}_{\mathfrak{ind}}(f)$, and $(b_2, b_1) = \mathfrak{b}_{\mathfrak{ind}}(b)$.

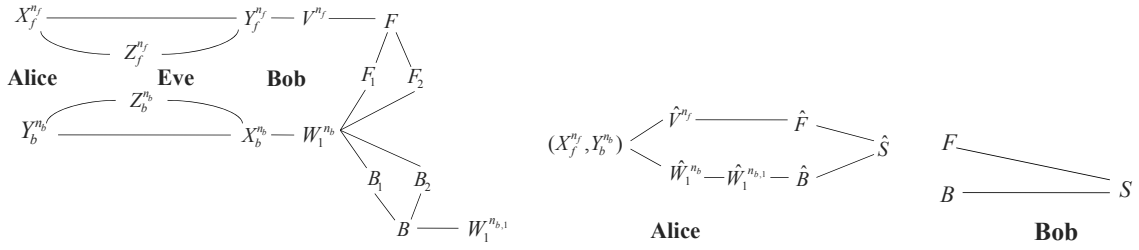
(xi) Let DMC_W be the DMC, $W_1 \to X_b$, that is specified by $P_{X_b|W_1}$.

Encoding. Alice selects an i.i.d. n_f-sequence $X_f^{n_f}$ and sends it over the forward DMBC. Bob and Eve receive $Y_f^{n_f}$ and $Z_f^{n_f}$, respectively. Bob finds a $V^{n_f} \in \mathcal{V}_\epsilon^{n_f}$ that is ϵ-jointly typical with $Y_f^{n_f}$ (w.r.t. P_{V,Y_f}), or returns a NULL if he fails. He selects independently a uniformly random $W_1^{n_{b,1}} \in \mathcal{W}_{1,\epsilon}^{n_{b,1}}$. He computes $F = \mathfrak{f}(V^{n_f})$, $B = \mathfrak{b}(W_1^{n_{b,1}})$, $(F_2, F_1) = \mathfrak{f}_{\mathfrak{ind}}(F)$, and $(B_2, B_1) = \mathfrak{b}_{\mathfrak{ind}}(B)$, and calculates $Enc(V^{n_f}, W_1^{n_{b,1}}) = (V^{n_f}, W_1^{n_b})$ using these variables. Next, Bob inputs $W_1^{n_b}$ to DMC_W to compute $X_b^{n_b}$, and sends $X_b^{n_b}$ over the backward DMBC. Alice and Eve receive $Y_b^{n_b}$ and $Z_b^{n_b}$, respectively.

Decoding. Alice searches through $\mathcal{V}_\epsilon^{n_f} \times \mathcal{W}_{1,\epsilon}^{n_{b,1}}$ and either finds a unique $(\hat{V}^{n_f}, \hat{W}_1^{n_{b,1}})$ that is (ϵ, n_f)-bipartite jointly typical to $(X_f^{n_f}, Y_b^{n_b})$ w.r.t. (P_{V,X_f}, P_{W_1,Y_b}), or returns a NULL.

Key Derivation. Bob computes $S = g(F, B)$. Alice computes $\hat{F} = \mathfrak{f}(\hat{V}^{n_f})$ and $\hat{B} = \mathfrak{b}(\hat{W}_1^{n_{b,1}})$, and then $\hat{S} = g(\hat{F}, \hat{B})$.

Fig. 3 shows the relationship between the random variables/sequences used in the ICC protocol. Two variables/sequences are connected by an edge if (1) they belong to input/outputs of the same DMBC, or (2) one is computed from the other by Alice or Bob using a (possibly randomized) function.



(a) Encoding and decoding (b) Key derivation by Alice (c) Key derivation by Bob

Fig. 3. The relation between the variables/sequences used in the ICC protocol for (a) encoding/decoding, (b) key derivation by Alice, and (c) key derivation by Bob

Uniformity Analysis: Proving (1a)

From AEP for P_V (see [3, Appendix A] for more details), and since F and V^{n_f} have the same distribution,

$$\forall f \in \mathcal{F},\ \Pr(F = f) \leq 2^{-\eta_f + 5N\epsilon}. \tag{30}$$

$$\Rightarrow \eta_f - 5N\epsilon \leq H(V^{n_f}) = H(F) \leq \eta_f, \tag{31}$$

Since $W_1^{n_{b,1}}$ (resp. B) is selected uniformly at random from $\mathcal{W}_{1,\epsilon}^{n_{b,1}}$ (resp. B) of size η_b

$$\forall b \in \mathcal{B},\ \Pr(B = b) = 2^{-\eta_b} \tag{32}$$

$$\Rightarrow H(W_1^{n_{b,1}}) = H(B) = \eta_b. \tag{33}$$

For every $i \in \{1, 2, \ldots, 2^\kappa\}$, the probability that $S = i$ equals to the probability that $(F, B) \in \mathcal{G}_i$. More specifically (see (28) and (29)),

$$\forall i:\ \Pr(S = i) = \sum_{f,b \in \mathcal{G}_i} \Pr(F = f \wedge B = b) \leq 2^\gamma 2^{-\eta_f + 5N\epsilon} 2^{-\eta_b} = 2^\gamma 2^{-\eta + 5N\epsilon} = 2^{-(\kappa - 5N\epsilon)}$$

$$\Rightarrow \frac{H(S)}{n_f + n_b} \geq \frac{\kappa - 5N\epsilon}{n_f + n_b} = R_{sk} - \delta, \qquad \delta \geq 5\epsilon. \tag{34}$$

Reliability Analysis: Proving (1b)

Since there are $\eta_f = n_f[I(V; Y_f) + \alpha]$ sequences in $\mathcal{V}_\epsilon^{n_f}$, from joint-AEP, with probability arbitrarily close to 1, there exists a $V^{n_f} \in \mathcal{V}_\epsilon^{n_f}$ that is ϵ-jointly typical with $Y_f^{n_f}$ (w.r.t. P_{V,Y_f}) and the encoding phase is successful. In the decoding phase, Alice needs to search through the 2^η words in $\mathcal{V}_\epsilon^{n_f} \times \mathcal{W}_{1,\epsilon}^{n_{b,1}}$,

where η is calculated as

$$\begin{aligned}\eta &= \eta_f + \eta_b \overset{(a)}{=} n_f(I(V;Y_f)+\alpha) + n_{b,1}(I(W_1;Y_b)-\beta)\\ &\overset{(b)}{=} n_f(I(V;Y_f)+\alpha) + n_b I(W_1;Y_b) - n_f(I(V_f;Y_f|X_f)+3\alpha) - n_{b,1}\beta\\ &\overset{(c)}{=} n_f(I(V;X_f,Y_f)+\alpha) + n_b I(W_1;Y_b) - n_f(I(V_f;Y_f|X_f)+3\alpha) - n_{b,1}\beta \qquad (35)\\ &= n_f I(V;X_f) + n_b I(W_1;Y_b) - 2n_f\alpha - n_{b,1}\beta\\ &< n_f I(V;X_f) + n_b I(W_1;Y_b) - 9N\epsilon. \qquad (36)\end{aligned}$$

Equality (a) follows from (26) and (27), equality (b) follows from (25), and equality (c) is due to the Markov chain $X_f \leftrightarrow Y_f \leftrightarrow V$. Since η is sufficiently smaller than $n_f I(V;X_f) + n_b I(W_1;Y_b)$, from AEP for bipartite sequences (see [3, Theorem 4]), there exist an encoding function $Enc(.)$ for which the decoding error probability becomes arbitrarily close to 0. This implies that

$$\Pr(\hat{S} \neq S) \leq \Pr\left((\hat{F},\hat{B}) \neq (F,B)\right) = \Pr\left((\hat{V}^{n_f},\hat{W}_1^{n_{b,1}}) \neq (V^{n_f},W_1^{n_{b,1}})\right) < \delta.$$

Secrecy Analysis: Proving (1c)

We shall show that the $H(S|Z_f^{n_f},Z_b^{n_b})$ is close to $H(S)$. For the quantities $H(F_2)$ and $H(B_2)$, we have (see [3, Appendix A] for more details)

$$\eta_{f,2} - 5N\epsilon \leq H(F_2) \leq \eta_{f,2}, \qquad (37)$$

$$\Rightarrow H(B_2) = \eta_{b,2}. \qquad (38)$$

We write $H(S|Z_f^{n_f},Z_b^{n_b})$ as

$$\begin{aligned}H(S|Z_f^{n_f},Z_b^{n_b}) &\geq H(S|F_2,B_2,Z_f^{n_f},Z_b^{n_b})\\ &= H(S,F,B|F_2,B_2,Z_f^{n_f},Z_b^{n_b}) - H(F,B|S,F_2,B_2,Z_f^{n_f},Z_b^{n_b})\\ &= H(F,B|F_2,B_2,Z_f^{n_f},Z_b^{n_b}) - H(F,B|S,F_2,B_2,Z_f^{n_f},Z_b^{n_b})\\ &= H(F,B|F_2,B_2) - I(F,B;Z_f^{n_f},Z_b^{n_b}|F_2,B_2) - H(F,B|S,F_2,B_2,Z_f^{n_f},Z_b^{n_b}). \qquad (39)\end{aligned}$$

The first term above is written as

The first term is written as

$$\begin{aligned}H(F,B|F_2,B_2) &= H(F|F_2,B_2) + H(B|F,F_2,B_2) \overset{(a)}{=} H(F|F_2) + H(B|B_2)\\ &\overset{(b)}{=} H(F) + H(B) - H(F_2) - H(B_2)\\ &\overset{(c)}{\geq} \eta_f - 5N\epsilon + \eta_b - \eta_{F,2} - \eta_{b,2}\\ &\overset{(d)}{\geq} n_f I(V;Y_f) - 2N\epsilon + n_{b,1}[I(W_1;Y_b)-\beta] - n_{b,2}I(W_2;Y_b) - n_{b,1}I(W_2;Y_b)\\ &\overset{(e)}{=} n_f I(V;X_f) + n_f I(V;Y_f|X_f) - 2N\epsilon + n_{b,1}I(W_1;Y_b) - n_b I(W_2;Y_b) - n_{b,1}\beta\\ &= n_f I(V;X_f) + n_f(I(V;Y_f|X_f)+3\alpha) + n_{b,1}I(W_1;Y_b) - n_b I(W_2;Y_b) - 3n_f\alpha - n_b\beta - 2N\epsilon\\ &\overset{(f)}{=} n_f I(V;X_f) + n_{b,2}I(W_1;Y_b) + n_{b,1}I(W_1;Y_b) - n_b I(W_2;Y_b) - 3n_f\alpha - n_b\beta - 2N\epsilon\\ &> n_f I(V;X_f) + n_b I(W_1;Y_b) - n_b I(W_2;Y_b) - 14N\epsilon\\ &\overset{(g)}{=} n_f I(V;X_f) + n_b I(W_1;Y_b|W_2) - 14N\epsilon \qquad (40)\end{aligned}$$

Equality (a) holds since B_2 and B are selected independently of F_2 and F, equality (b) holds since F_2 and B_2 are deterministic functions of F and B, respectively (the encoding phase), inequality (c) follows from (31), (33), (37), and (38), equality (d) follows from (26) and (27), equality (e) is due to the Markov chain $X_f \leftrightarrow Y_f \leftrightarrow V$, equality (f) follows from (25), and equality (g) is due to the Markov chain $W_2 \leftrightarrow W_1 \leftrightarrow Y_b$.

The second term in (39) is written as

$$\begin{aligned} I(F,B;Z_f^{n_f},Z_b^{n_b}|F_2,B_2) &= I(F,B;Z_f^{n_f}|F_2,B_2) + I(F,B;Z_b^{n_b}|Z_f^{n_f},F_2,B_2) \\ &\overset{(a)}{=} I(V^{n_f},B;Z_f^{n_f}|F_2,B_2) + I(F,B;Z_b^{n_b}|Z_f^{n_f},F_2,B_2) \\ &\overset{(b)}{\leq} I(V^{n_f};Z_f^{n_f}) + I(F,B;Z_b^{n_b}|F_2,B_2) \\ &\overset{(c)}{=} I(V^{n_f};Z_f^{n_f}) + H(Z_b^{n_b}|F_2,B_2) - H(Z_b^{n_b}|F,B) \\ &\overset{(d)}{\leq} n_f I(V;Z_f) + n_b[H(Z_b|W_2) - H(Z_b|W_1)] \\ &\overset{(e)}{\leq} n_f I(V;Z_f) + n_b I(W_1;Y_b|W_2) \end{aligned} \tag{41}$$

Inequality (a) holds because $V^{n_f} = \mathfrak{f}^{-1}(F)$ (the key derivation phase), equality (b) is due to the Markov chains $(F_2,B_2) \leftrightarrow (V^{n_f},B) \leftrightarrow Z_f^{n_f}$, $B \leftrightarrow V^{n_f} \leftrightarrow Z_f^{n_f}$ and $Z_f^{n_f} \leftrightarrow F \leftrightarrow Z_b^{n_b}$, equality (c) holds since F_2 and B_2 are deterministic functions of F and B, equality (d) follows from AEP, and equality (e) is due to the Markov chain $W_2 \leftrightarrow W_1 \leftrightarrow Z_b$.

It remains to calculate $H(F,B|S,F,B,Z_f^{n_f},Z_b^{n_b})$, i.e., the third term in (39). From (vii), knowing $S=i$ gives the partition $\mathcal{G}_i$ that F,B belongs to; further, knowing $F_2=f_2$ and $B_2=b_2$ gives the parity-check sequence $w_{2,f_2,b_2}^{n_{b,1}} \in \mathcal{P}_2$ which is used in the encoding phase (see (viii)). Define the codebook

$$\mathcal{C}_i^e = \{v^{n_f}, w_1^{n_b} : \ (\mathfrak{f}(v^{n_f}),b) \in \mathcal{G}_i, \ w_1^{n_b} = Enc(\mathfrak{f}(v^{n_f}),b), \ F_2=f_2, \ B_2=b_2\}.$$

Given $S=i, Z_f^{n_f}$, and $Z_b^{n_b}$, one can search all the codewords in $\mathcal{C}_i^e$ and return a unique $\check{V}^{n_f}, \check{W}_1^{n_b} \in \mathcal{C}_i^e$ that is (ϵ,n_f)-bipartite jointly typical to $(Z_f^{n_f},Z_b^{n_b})$ w.r.t. (P_{V,Z_f},P_{W_1,Z_b}); otherwise return a NULL. From (vii), $|\mathcal{G}_i| = 2^{\gamma}$, and so $|\mathcal{C}_i^e| = 2^{\gamma-\eta_2}$, where η_2 is given in (28). We first calculate η which is used in the calculation of $\gamma - \eta_2$.

$$\begin{aligned} \eta &= \eta_f + \eta_b \\ &= n_f(I(V;Y_f)+\alpha) + n_{b,1}I(W_1;Y_b) - n_b\beta \\ &= n_f I(V;X_f) + n_f(I(V;Y_f|X_f)+3\alpha) + n_{b,1}I(W_1;Y_b) - 2n_f\alpha - n_b\beta \\ &= n_f I(V;X_f) + n_b I(W_1;Y_b) - 3n_f\alpha. \end{aligned}$$

$\gamma - \eta_2$ is written as

$$\begin{aligned}
\gamma - \eta_2 &\overset{(a)}{=} \eta - (n_f + n_b)R_{sk} - \eta_{f,2} - \eta_{b,2} \\
&\overset{(b)}{\leq} n_f I(V; X_f) + n_b I(W_1; Y_b) - 3n_f\alpha + n_f[I(V; Z_f) - I(V; X_f)] \\
&\quad + n_b[I(W_1; Z_b|W_2) - I(W_1; Y_b|W_2)] - n_{b,2} I(W_2; Y_b) - n_{b,1} I(W_2; Y_b) \\
&= n_b I(W_1; Y_b) - 3n_f\alpha + n_f I(V; Z_f) + n_b[I(W_1; Z_b|W_2) - I(W_1; Y_b|W_2)] - n_b I(W_2; Y_b) \\
&\overset{(c)}{=} n_f I(V; Z_f) + n_b I(W_1; Z_b|W_2) - 3n_f\alpha \\
&\overset{(d)}{<} n_f I(V; Z_f) + n_b I(W_1; Z_b) - 9N\epsilon.
\end{aligned}$$

Equality (a) follows from (28) and (29), inequality (b) follows from the definition of R_{sk} in (22), equality (c) is due to the Markov chain $W_2 \leftrightarrow W_1 \leftrightarrow Y_b$, and inequality (d) is due to the Markov chain $W_2 \leftrightarrow W_1 \leftrightarrow Z_b$. Since $\gamma - \eta_2$ is sufficiently smaller than $n_f I(V; Z_f) + n_b I(W_1; Z_b)$, from joint-AEP for bipartite sequences [3, Theorem 4], for an appropriately chosen partition $\{\mathcal{G}_i\}_{i=1}^{2^\kappa}$, the decoding error probability becomes arbitrarily close to 0, i.e., given $(S, F_2, B_2, Z_f^{n_f}, Z_b^{n_b})$,

$$\Pr\left((\check{V}^{n_f}, \check{W}_1^{n_b}) \neq (V^{n_f}, W_1^{n_b})\right) < 2\epsilon.$$

Letting $\check{F} = \mathfrak{f}(\check{V}^{n_f})$ and $\check{B}, \check{F} = Enc(\check{W}_1^{n_b})$, we have

$$\Pr\left((\check{F}, \check{B}) \neq (F, B)\right) < 2\epsilon.$$

Using Fano's inequality [6] results in

$$H(F, B|S, F, B, Z_f^{n_f}, Z_b^{n_b}) \leq H(F, B|\check{F}, \check{B}) < h(2\epsilon) + 2\epsilon\eta, \tag{42}$$

where $h(\epsilon) = -\epsilon\log(\epsilon) - (1-\epsilon)\log(1-\epsilon)$ is the binary entropy function. Applying (40)-(42) in (39) gives

$$\begin{aligned}
H(S|Z_f^{n_f}, Z_b^{n_b}) &> n_f[I(V; X_f) - I(V; Z_f)] + n_b[I(W_1; Y_b|W_2) - I(W_1; Z_b|W_2)] \\
&\quad - 14N\epsilon - h(2\epsilon) - 2\epsilon\eta \\
&= (n_f + n_b)R_{sk} - 14N\epsilon - h(2\epsilon) - 2\epsilon\eta \\
&\geq H(S) - 14N\epsilon - h(2\epsilon) + 2\epsilon\eta,
\end{aligned}$$

where the last inequality follows from (34). This implies that by appropriate selection of ϵ for an arbitrarily small δ, we will have

$$\frac{H(S|Z_f^{n_f}, Z_b^{n_b})}{H(S)} > 1 - \delta.$$

B. Proof of Proposition 1

From (2a) and the independence of the two DMCs in the sd-2DMBC setup (see Definitions 4 and 5), $V_f \leftrightarrow Y_f \leftrightarrow X_f \leftrightarrow Z_f$ forms a Markov chain, and so we write (3a) and (3c) as

$$R_{s1}^A = I(V_f; X_f, Z_f) - I(V_f; Z_f) = I(V_f; X_f|Z_f), \tag{43}$$

$$R_{s1}^B = I(V_b; X_b, Z_b) - I(V_b; Z_b) = I(V_b; X_b|Z_b). \tag{44}$$

From Definition 4 and the second Markov chain in (2a), there exist $\tilde{Y}_b$ and $\tilde{Z}_b$ such that one of the Markov chains

$$W_{2,b} \leftrightarrow W_{1,b} \leftrightarrow X_b \leftrightarrow \tilde{Y}_b \leftrightarrow \tilde{Z}_b, \text{ or} \tag{45a}$$

$$W_{2,b} \leftrightarrow W_{1,b} \leftrightarrow X_b \leftrightarrow \tilde{Z}_b \leftrightarrow \tilde{Y}_b \tag{45b}$$

hold, and

$$\begin{aligned} &I(X_b;Y_b) = I(X_b;\tilde{Y}_b), \quad I(X_b;Z_b) = I(X_b;\tilde{Z}_b) \\ &I(W_{1,b};Y_b|W_{2,b}) = I(W_{1,b};\tilde{Y}_b|W_{2,b}), \\ &I(W_{1,b};Z_b|W_{2,b}) = I(W_{1,b};\tilde{Z}_b|W_{2,b}). \end{aligned}$$

Hence, we write (3b) as

$$\begin{aligned} R_{s2}^A &= I(W_{1,b};\tilde{Y}_b|W_{2,b}) - I(W_{1,b};\tilde{Z}_b|W_{2,b}) \\ &\le I(W_{1,b};\tilde{Y}_b|\tilde{Z}_b,W_{2,b}) \overset{(a)}{\le} I(X_b;\tilde{Y}_b|\tilde{Z}_b) \\ &= [I(X_b;\tilde{Y}_b) - I(X_b;\tilde{Z}_b)]_+ = [I(X_b;Y_b) - I(X_b;Z_b)]_+. \end{aligned} \tag{46}$$

Inequality (a) follows from (45). More precisely, if (45a) holds the inequality is easily satisfied, and if (45b) holds both sides equal zero. It is easy to see that equality in (46) holds by choosing $W_{2,b} = 1$ and $W_{1,b}$ to be X_b or 1, in the case of (45a) or (45b), respectively. In analogy to the above, we have

$$R_{s2}^B \le [I(X_f;Y_f) - I(X_f;Z_f)]_+, \tag{47}$$

where equality holds for some $W_{2,f}$ and $W_{1,f}$. By replacing $R_{s1}^A, R_{s2}^A, R_{s1}^B$, and R_{s2}^B in (5) and (6) with the above-obtained quantities, (4) is simplified to (14).

C. Proof of Theorem 2

We let Alice be the party who sends i.i.d. variables. The other case follows by symmetry. We use Lemma 1 to reduce a multi-round SKE protocol to a two-round one, and then give the highest rate that a two-round protocol can achieve.

Lemma 1: When Alice can only send i.i.d. variables, the secret-key capacity is achieved by a two-round SKE protocol whose initiator is Alice.

Proof: Let Π be a t-round SKE protocol that achieves the secret-key capacity under the above condition.

Case 1: Alice sends in odd rounds. In any (odd) round r, Alice's sent sequence $X_f^{:r}$ is independent of her view in round $r-1$, and hence she could compute it in the first communication round. Besides, sending this sequence in the first round does not affect the distribution of Bob's and Eve's received sequences ($Y_f^{:r}$ and $Z_f^{:r}$) since the channels are memoryless. Obviously Bob can compute $X_b^{:r}$ for any even r as before. Hence, we can convert the protocol Π into Π' in which Alice sends the whole $||_{(odd)r\le t}\left[X_f^{n_{f,r}:r}\right]$ in the first round such that all the communicated sequences and the final key in Π and Π' have the same joint probability distribution, i.e., if the same randomness is chosen by Alice, Bob, and the 2DMBC in the execution of Π and Π', then all the communicated sequences and the final key are identical. Now, Bob can send the whole $||_{(even)r\le t}\left[X_b^{n_{b,r}:r}\right]$ in the second round without affecting the joint distribution of the

sequences. We refer to this last protocol as Π'' which is a two-round protocol with Alice as the initiator such that the communicated sequences and the key have the same joint distribution as in Π. Hence Π'' achieves the secret-key capacity.

Case 2: Alice sends in even rounds. Using a similar argument to that of Case 1, we reach a three-round protocol Π'' with Bob as the initiator: Bob sends $X_b^{n_{b,1}:1}$ in the first round, Alice sends $||_{(even)r\leq t}\left[X_f^{n_{f,r}:r}\right]$ in the second round, and Bob sends $||_{(odd)3\leq r\leq t}\left[X_b^{n_{b,r}:r}\right]$ in the third round. Since the communicated sequence in the first round is not used to calculate the second round communicated sequences, Bob can send $X_b^{n_{b,1}:1}$ in the third round without affecting the distribution of the sequences in the protocol Π''. This gives a two-round communication protocol with Alice as the initiator that achieves the capacity. ■

Now, consider a two-round SKE protocol as depicted in Fig. 4 in which Alice sends a sequence of i.i.d. variables $X_f^{n_f}$ in the first round. Since the channels are memoryless and independent, Bob and Eve receive sequences of i.i.d. variables $Y_f^{n_f}$ and $Z_f^{n_f}$ and $Y_f \leftrightarrow X_f \leftrightarrow Z_f$ is a Markov chain. This can be seen as the Discrete Memoryless Multiple Source (DMMS) (Y_f, X_f, Z_f) between Bob, Alice, and Eve, respectively and the DMBC $X_b \rightarrow (Y_b, Z_b)$ from Bob to Alice and Bob. When the DMMS and DMBC satisfy the degradedness condition $Y_f \leftrightarrow X_f \leftrightarrow Z_f$ and $X_b \leftrightarrow Y_b \leftrightarrow Z_b$, [7] proves an upper bound on the secret-key capacity that coincides with the lower bound in (14). However, the proof in [7] can not be directly applied to our problem due to the "stochastic" degradedness of the (backward) DMBC. We give the following argument to upper bound the highest achievable rate R_{sk} for an arbitrarily small $\delta > 0$ as in (1).

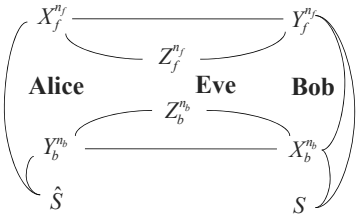


Fig. 4. The relations between variables/sequences in two-round SKE when Alice starts the protocol and Bob calculates the key

The views of the parties at the end of the second round are $View_A = (X_f^{n_f}, Y_b^{n_b})$, $View_B = (Y_f^{n_f}, X_b^{n_b})$, and $View_E = (Z_f^{n_f}, Z_b^{n_b})$. Using Fano's inequality for (1b), we have

$$H(S|View_A) \leq H(S|\hat{S}) < h(\delta) + \delta H(S), \tag{48}$$

Furthermore, (1c) gives

$$I(S; View_E) = H(S) - H(S|View_E) \leq \delta H(S). \tag{49}$$

In the following, we omit the length of the sequences, $X_f^{n_f}, Y_f^{n_f}, Z_f^{n_f}$ and $X_b^{n_b}, Y_b^{n_b}, Z_b^{n_b}$ from the superscripts, instead use bold to denote them. $H(S)$ is upper bounded as

$$\begin{aligned}
H(S) &= I(S; View_A) + H(S|View_A) \\
&\overset{(a)}{\leq} I(S; View_A) - I(S; View_E) + h(\delta) + 2\delta H(S) \\
&\leq I(S; View_A|View_E) + h(\delta) + 2\delta H(S) \\
\Rightarrow (1-2\delta)H(S) - h(\delta) &\leq I(S; View_A) - I(S; View_E) \\
&= I(S; \mathbf{Y}_b) + I(S; \mathbf{X}_f|\mathbf{Y}_b) - I(S; \mathbf{Z}_f, \mathbf{Z}_b) \\
&= I(S; \mathbf{Y}_b) + I(S; \mathbf{X}_f, \mathbf{Z}_f|\mathbf{Y}_b) - I(S; \mathbf{Z}_f, \mathbf{Z}_b) \\
&= I(S; \mathbf{Y}_b) + I(S; \mathbf{Z}_f|\mathbf{Y}_b) + I(S; \mathbf{X}_f|\mathbf{Z}_f, \mathbf{Y}_b) - I(S; \mathbf{Z}_f, \mathbf{Z}_b) \\
&= [I(S; \mathbf{Z}_f, \mathbf{Y}_b) - I(S; \mathbf{Z}_f, \mathbf{Z}_b)] + [I(S; \mathbf{X}_f|\mathbf{Z}_f, \mathbf{Y}_b)], \qquad (50)
\end{aligned}$$

where inequality (a) follows from (48) and (49). We separately discuss the two terms in (50). Note that $(S, \mathbf{Z}_f) \leftrightarrow \mathbf{X}_b \leftrightarrow (\mathbf{Y}_b, \mathbf{Z}_b)$ is a Markov chain. If the backward DMBC is stochastically degraded in favor of Z_b, the first term is at most zero; otherwise, letting $X_b \leftrightarrow \tilde{Y}_b \leftrightarrow \tilde{Z}_b$ (see Definition 4), we have

$$\begin{aligned}
I(S; \mathbf{Z}_f, \mathbf{Y}_b) - I(S; \mathbf{Z}_f, \mathbf{Z}_b) &= I(S; \mathbf{Z}_f, \tilde{\mathbf{Y}}_b) - I(S; \mathbf{Z}_f, \tilde{\mathbf{Z}}_b) \\
&= I(S; \mathbf{Z}_f, \tilde{\mathbf{Y}}_b, \tilde{\mathbf{Z}}_b) - I(S; \mathbf{Z}_f, \tilde{\mathbf{Z}}_b) I(S; \tilde{\mathbf{Y}}_b|\mathbf{Z}_f, \tilde{\mathbf{Z}}_b) \\
&\leq I(S, \mathbf{Z}_f; \tilde{\mathbf{Y}}_b|\tilde{\mathbf{Z}}_b) = I(S, \mathbf{Z}_f; \tilde{\mathbf{Y}}_b) - I(S, \mathbf{Z}_f; \tilde{\mathbf{Z}}_b) \\
&= I(S, \mathbf{Z}_f; \mathbf{Y}_b) - I(S, \mathbf{Z}_f; \mathbf{Z}_b) \overset{(a)}{\leq} n_b[I(W_b; Y_b) - I(W_b; Z_b)] \\
&\overset{(b)}{\leq} n_b[I(X_b; Y_b) - I(X_b; Z_b)]_+. \qquad (51)
\end{aligned}$$

Inequality (a) follows from the results of message transmission over single DMBCs (e.g., [4, Section V]), where the conditional distribution $P_{Y_b, Z_b|X_b}$ corresponds to the backward DMBC and W_b is an RV that satisfies the Markov chain $W_b \leftrightarrow X_b \leftrightarrow (Y_b, Z_b)$. Inequality (b) is due to the degradedness of the backward DMBC. Letting J be an independent random variable uniformly distributed over $\{1, 2, \ldots, n_f\}$, we write the second term in (50) as

$$\begin{aligned}
I(S; \mathbf{X}_f|\mathbf{Z}_f, \mathbf{Y}_b) &\leq I(S, \mathbf{Y}_b; \mathbf{X}_f|\mathbf{Z}_f) \\
&\overset{(a)}{=} I(S, \mathbf{Y}_b; \mathbf{X}_f) - I(S, \mathbf{Y}_b; \mathbf{Z}_f) \\
&\overset{(b)}{=} \sum_{i=1}^{n_f} I(S, \mathbf{Y}_b; X_{f,i}|Z_{f,i+1}^{n_f}, X_f^{i-1}) - I(S, \mathbf{Y}_b; Z_{f,i}|Z_{f,i+1}^{n_f}, Z_f^{i-1}) \\
&\overset{(c)}{=} \sum_{i=1}^{n_f} I(S, \mathbf{Y}_b; X_{f,i}|Z_{f,i}, Z_{f,i+1}^{n_f}, X_f^{i-1}) \\
&= n_f I(S, \mathbf{Y}_b; X_{f,J}|Z_{f,J}, Z_{f,J+1}^{n_f}, X_f^{J-1}, J) \\
&\leq n_f I(S, \mathbf{Y}_b, Z_{f,J+1}^{n_f}, X_f^{J-1}, J; X_{f,J}|Z_{f,J}). \qquad (52)
\end{aligned}$$

Equality (a) is due to the Makov chain $\mathbf{Z}_f \leftrightarrow \mathbf{X}_f \leftrightarrow (S, \mathbf{Y}_b)$, equality (b) follows from the chain rule for difference between mutual information (see e.g., [4, Section V]), and equality (c) is due to the Markov chain $Z_{f,i} \leftrightarrow X_{f,i} \leftrightarrow (S, \mathbf{Y}_b)$.

Now, letting $V_f = (S, \mathbf{Y}_b, Z_{f,J+1}^{n_f}, X_f^{J-1}, J)$, $X_f = X_{f,J}$, $Y_f = Y_{f,J}$ and $Z_f = Z_{f,J}$, the conditional distribution $P_{Y_f.Z_f|X_f}$ corresponds to the forward DMBC, the Markov chain $Z_f \leftrightarrow X_f \leftrightarrow Y_f \leftrightarrow V_f$ is satisfied, and we have

$$I(S; \mathbf{X}_f | \mathbf{Z}_f, \mathbf{Y}_b) \leq n_f I(V_f; X_f | Z_f). \tag{53}$$

Using the quantities of (51) and (53) in the calculation of (50), $H(S)$ is upper bounded as

$$\begin{aligned} H(S) \leq & \frac{n_f I(V_f; X_f|Z_f) + n_b [I(X_b; Y_b) - I(X_b; Z_b)]_+ + h(\delta)}{(1-2\delta)} \\ = & n_f I(V_f; X_f|Z_f) + n_b [I(X_b; Y_b) - I(X_b; Z_b)]_+, \end{aligned} \tag{54}$$

where the last equality holds since δ is arbitrarily small. This together with (1a) proves the argument in (15), and the condition in (15) is proven as follows.

$$\begin{aligned} n_b I(X_b; Y_b) \geq & I(\mathbf{X}_b; \mathbf{Y}_b) \overset{(a)}{\geq} I(\mathbf{Y}_f; \mathbf{Y}_b) \\ & = I(\mathbf{Y}_b, S; \mathbf{Y}_f) - I(S; \mathbf{Y}_f | \mathbf{Y}_b) \geq I(\mathbf{Y}_b, S; \mathbf{Y}_f) - H(S|\mathbf{Y}_b) \\ & = I(\mathbf{Y}_b, S; \mathbf{Y}_f) - H(S|\mathbf{Y}_b, \mathbf{X}_f) - I(S; \mathbf{X}_f | \mathbf{Y}_b) \\ & \overset{(b)}{\geq} I(\mathbf{Y}_b, S; \mathbf{Y}_f) - h(\delta) - \delta H(S) - I(S; \mathbf{X}_f | \mathbf{Y}_b) \\ & \overset{(c)}{\geq} I(\mathbf{Y}_b, S; \mathbf{Y}_f) - I(\mathbf{Y}_b, S; \mathbf{X}_f) \\ & \overset{(d)}{=} \sum_{i=1}^{n_f} I(\mathbf{Y}_b, S, X_f^{i-1}, Y_{f,i+1}^{n_f}; Y_{f,i}) - I(\mathbf{Y}_b, S, X_f^{i-1}, Y_{f,i+1}^{n_f}; X_{f,i}) \\ & \overset{(e)}{=} \sum_{i=1}^{n_f} I(\mathbf{Y}_b, S, X_f^{i-1}, Y_{f,i+1}^{n_f}; Y_{f,i} | X_{f,i}) \\ & \overset{(f)}{\geq} \sum_{i=1}^{n_f} I(\mathbf{Y}_b, S, X_f^{i-1}, Z_{f,i+1}^{n_f}; Y_{f,i} | X_{f,i}) \\ & = n_f I(\mathbf{Y}_b, S, X_f^{J-1}, Z_{f,J+1}^{n_f}; Y_{f,J} | X_{f,J}, J) = n_f I(V_f; Y_f | X_f) - n_f I(J; Y_f | X_f) \\ & \overset{(g)}{=} n_f I(V_f; Y_f | X_f). \end{aligned} \tag{55}$$

Inequality (a) is due to the Markov chain $\mathbf{Y}_f \leftrightarrow \mathbf{X}_b \leftrightarrow \mathbf{Y}_b$; inequality (b) follows from (48); inequality (c) holds since δ is arbitrarily small and so $h(\delta) + \delta H(S)$ is negligible compared to the other quantities; equality (d) follows from the chain rule for difference between mutual information; equality (e) is due to the Markov chain $X_{f,i} \leftrightarrow Y_{f,i} \leftrightarrow (\mathbf{Y}_b, S, X_f^{i-1}, Y_{f,i+1}^{n_f})$; inequality (f) is due to the Markov chain $Z_{f,i+1}^{n_f} \leftrightarrow Y_{f,i+1}^{n_f} \leftrightarrow Y_{f,i}$, and equality (g) holds since $Y_{f,J}$ is (i.i.d.) independent of J.

One can prove (16) by symmetry. This implies that, under the condition of this theorem, equality in (14) holds.

V. Conclusion

We extended the results of SKE in the 2DMBC setup in the following two cases. When both DMBCs have secrecy potential, we proposed the interactive channel coding (ICC) protocol and proved that it achieves the lower bound. When both DMBCs are stochastically degraded with independent channels (so called sd-2DMBC), we provided a simplified expression for the lower bound, and proved that this

lower bound is tight under the condition that one of the parties sends only i.i.d variables. Obtaining a single-letter characterization or even a tighter upper bound for the secret-key capacity in the sd-2DMBC setup remains as future work.

REFERENCES

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. Part I: secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121-1132, Jul. 1993.

[2] R. Ahlswede and N. Cai, "Transmission, identification, and common randomness capacities for wire-tape channels with secure feedback from the decoder," book chapter in General Theory of Information Transfer and Combinatorics, LNCS 4123, pp. 258-275, 2006.

[3] H. Ahmadi and R. Safavi-Naini, "Secret Key Establishment over a Pair of Independent Broadcast Channels", arXiv:1001.3908, available online on the arXiv preprint server.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339-348, May 1978.

[5] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, pp. 344366, 2000.

[6] R. G. Gallager, *Information Theory and Reliable Communication*, New York: Wiley, 1968.

[7] A. Khisti, S. Diggavi, G. Wornell, "Secret key generation using correlated sources and noisy channels," *IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 1005-1009, 2008.

[8] J. Körner and K. Marton, "Comparison of two noisy channels," *Transactions of the Hungarian Colloquium on Information Theory*, Keszthely, pp. 411-423, 1977.

[9] L. Lai, H. El Gamal, and V. Poor, "The wiretap channel with feedback: encryption over the channel," *IEEE Trans. Inf. Theory*, vol. IT-54, no. 11, pp. 5059-5067, 2008.

[10] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451-456, Jul. 1978.

[11] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733-742, May 1993.

[12] V. Prabhakaran, K. Eswaran and K. Ramchandran, "Secrecy via Sources and Channels - A Secret Key - Secret Message Rate Trade-off Region," *IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 1010-1014, 2008.

[13] E. Tekin and A. Yener, "The general Gaussian multiple access channel and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. IT-54, no. 6, pp. 2735-2751, 2008.

[14] A. D.Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1367, Oct. 1975.